CLAIMS

1. A method of communication over a wireless communications network, the network comprising at least first and second transceivers, linked by wireless communication paths, each path including at least one repeater disposed within the network for the propagation of messages, the method comprising the steps of:

transmitting a plurality of signals that make up a message, through the network to the second transceiver; and

determining from received signals whether one or more of the signals has undergone tampering.

2. The method of claim 1 further including the step of asserting a security breach condition in response to the determination of a tampering condition.

3. The method of claim 1 wherein the signals of the message are divided and sent across two communication paths.

4. The method of claim 3 wherein the signals sent on the same communication path are separated in time.

5. The method of claim 1 wherein the signals sent on one communication path are also sent on another communication path.

6. The method of claim 5 wherein the signals are sent on both communication paths at the same time or at different times.

7. The method of claim 3 or claim 5 wherein the determining step compares the signals received on the two communication paths.

8. The method of claim 3 or claim 5 wherein the determining step identifies signal tampering if the second transceiver receives signals on one communication path only.

9. The method of claim 5 wherein the determining step identifies signal tampering if the signals received on one communication path do not match the signals received on the other communication path.

10. The method of claim 3 wherein the determining step identifies tampering if relative delays between signal arrival times deviate from an expected delay.

11. The method of claim 3, wherein the determining step identifies signal tampering if the received signals indicate at least one signal is missing.

12. The method of claim 1 wherein one of the communication paths is configured to be relatively insecure and vulnerable to security breaches.

13. The method of claim 12 wherein the determining step compares the signals received on the insecure communication path to signals received on another communication path.

14. The method of claim 1 wherein at least some of the signals of the message are adapted to contain spurious information.

15. The method of claim 14 wherein the determining step comprises identifying said spurious signals and determining whether they originate from an authorised device or an unauthorised device.

16. The method of claim 15 in which the step of determining whether spurious signals originate from an authorised device or an unauthorised device comprises checking a condition of use.

17. The method of claim 1, comprising the further steps of:

configuring, prior to transmitting, one of the communication paths to be insecure and vulnerable to security breaches; and

adapting, at least some of the signals of the message to contain spurious information, wherein the transmitting step only sends the spurious signals on the insecure communication path.

18. The method of claim 14 in which the spurious information is inserted by a repeater.

19. The method of claim 2 in which the step of asserting a security breach comprises the step of asserting an alarm condition.

20. The method of claim 19 in which the step of asserting a security breach comprises the step of inhibiting message transmission between at least some devices on the network.

21. A receiver for receiving messages over a wireless communications network and for detecting tampering of the signals in the wireless network, comprising:

means for receiving a plurality of signals that make up a message, from the network;

means for determining from the received signals whether one or more of the signals has undergone tampering.

22. A method for detecting the presence of an unauthorised device attempting to connect to a network, comprising the steps of:

transmitting a first message, onto a network, which first message includes spurious data which purports to be data that enables or maintains connection of a device to the network; and

detecting subsequent use of that data to identify an unauthorised attempt to connect to the network.

23. The method of claim 22 in which the step of transmitting the first message comprises sending the message from a first device over the network and back to the first device.

24. The method of claim 22 in which the step of transmitting a message including spurious data comprises sending the message from a first device to a second device according to a predetermined plan.

25. The method of claim 22 further including the step of transmitting a second message that includes spurious data that purports to be a response from a device connecting or connected to the network in response to the first message.

26. The method of claim 25 in which the first and second messages are transmitted by the same device.

27. The method of any one of claims 22 to 26 in which the first message is transmitted from, or is repeated by, a device in a relatively insecure location.

28. The method of any one of the claims 22 to 27 in which a device transmitting the first message is a network controller.

29. A device for use on a network, the device comprising:

a transmitter for transmitting a first message onto the network, which first message includes spurious data which purports to be data that enables or maintains connection of a device to the network; and

detection means for detecting subsequent use of that data, by another device, to identify an unauthorised attempt to connect to the network.